



Product Summary

Automated Fraud Detection Module (AFD™) v1.28

The AFD™ provides an organisation with the ability to perform its own fraud and risk profiling in one of its most vulnerable areas: the Purchasing and Procurement function.

Using tests based on real-life fraud investigations, the AFD™ uses information from three key internal data sources: suppliers, employees and invoice transactions, to perform a rigorous series of analyses which may be fine tuned at run time. The AFD™ also identifies anomalous transactions and “odd” relationships by comparing the organisation’s data against specialist, external, data sources such as, accommodation addresses, financial details of factoring agents, and UK prisons. The system includes a risk scoring and weighting mechanism automatically highlighting those suppliers with the greatest potential exposure.

The AFD™ enables an organisation to implement a proactive, fraud-prevention strategy in accordance with the requirements of the US Sarbanes-Oxley Act and the best practices of UK corporate governance.

NB. Compliance with local data protection legislation is required before the personnel verification element of this solution can be implemented.

Accounts Payable Analyser (APA™) v1.0

The APA™ provides an unrivalled and self-funding insight into the Accounts Payable function. The duplicate invoice reports provide the organisation with the ability to make substantial recoveries from overpayments to their suppliers. In addition, the supplier and data integrity reports allow the client to implement improved controls by increasing the visibility of supplier relationships, improving the quality and accuracy of supplier information (and hence the ability to verify this information) and reducing the number of obsolete supplier records.

The APA™ produces over 175 detailed, purchase ledger reports spanning data integrity; invoice, cash and supplier management; and historic cost recovery. These reports include:

- Integrity reports to identify missing or invalid data within the client’s primary accounting files
- Suppliers with anomalous invoicing and (or) payment patterns;
- Suppliers with duplicate details;
- Duplicate invoice reports, and
- VAT analysis.

Corporate Procurement Card Profiler (CPCP™) v1.0

Corporate procurement cards are increasingly being used to facilitate the purchase of low-value, ad hoc items without the extended procurement process. Card providers protect the organisation from external frauds such as “cloning” and “skimming” but fail to recognise or report deliberate abuse by the authorised cardholder.

The CPCP™ is designed to provide a cost-effective mechanism for identifying transactions by authorised cardholders who deliberately attempt to by-pass internal controls. For example, a cardholder colluding with a store to split a £5,000 purchase over five days, each with a single £1,000 transaction. Other forms of corporate procurement card abuse include two or more authorised cardholders splitting a single purchase over several different cards. Standard reports include:

- Several different levels of duplicate transaction detection;
- The identification of sequential transactions to highlight split purchases;
- Summary management information to enable senior managers to quickly and easily identify unusual purchasing patterns; and
- The failure of the card issuing companies to adequately implement “blocked merchant categories”, and hence allow purchases by the cardholder of items not sanctioned by the organisation. For example, the use of a procurement card to access pornographic internet sites.



IDM D.A.T.A. Solutions Limited

Personnel Verification Profiler (PVP™) v1.0

Industry bodies such as the UK Fraud Advisory Panel recognise that in cases where fraud has been reported and investigated, the main contributory factors were:

- a breach of trust by one or more employees; and
- an abuse or avoidance of internal controls.

Since employees are responsible for around three-quarters of reported frauds, IDS has developed a series of profiles that identify situations where the organisation is at greater risk due to unusual employee relationships. These profiles include matching data between:

- employees and suppliers (or clients);
- employees and disqualified directors' details held by Companies House;
- employees operating from known mail box and accommodation addresses; and
- three way relationships between employees, their next-of-kin and suppliers (or clients).

NB. Compliance with local data protection legislation will be required to implement this solution.

Reference File Profiler (RFP™) v1.0

Many organisations now have a regulatory obligation to ensure that they implement appropriate monitoring systems to identify possible money-laundering transactions and other categories of unusual transactions.

IDS' Reference File Profiler allows an organisation to verify a specific set of computer records against an external reference set. This may be performed at several levels such as matching company names, addresses, financial banking details, etc. against known black listed entities. For example, an organisation may wish to verify that proposed payments to external third parties do not include known illegal organisations as defined, by the US Treasury, known as the "OFAC" list.

IDS' practical approach to detecting unusual transactions ensures that organisations can implement a modular, transaction-monitoring system, evaluating and fine-tuning each transaction profile before developing the next one. The cost of implementing such is generally a fraction of the cost of many established money-laundering systems.

Telecoms Billing Verifier (TBV™) v1.0

Telecommunications costs for many organisations can run into many hundreds of thousand of pounds each year. With the rapidly changing market place, telecoms charges and tariffs change on an almost monthly basis and should be constantly reviewed. The Telecoms Billing Verifier ("TBV™") uses current rates and tariffs from the service providers' web sites to recalculate their telecoms bills and verifies their charges.

The TBV™ consists of two major components:

- a price table maintenance suite, which uses information concerning charges for calls obtained from the service providers on a regular basis; and
- a bill verification suite, which recalculates the cost of calls, based on the information included in the bill (destination numbers, start dates and times and call durations) and the pricing schemes applicable to the lines from which calls have been made.

IDM D.A.T.A. Solutions Limited
February 2005